UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/720,329	11/24/2003	Weng-Chin Yung	6533/53793	4304

30505 7590 07/11/2007

LAW OFFICE OF MARK J. SPOLYAR
2200 CESAR CHAVEZ STREET
SUITE 8
SAN FRANCISCO, CA 94124

EXAMINER	
KOLETOWO, RASHEEDAT	

ART UNIT	PAPER NUMBER
2609	

MAIL DATE	DELIVERY MODE
07/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/720,329	Applicant(s) YUNG ET AL.	
	Examiner Rasheedat O. Koletowo	Art Unit 2609	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33* is/are rejected.

7)☒ Claim(s) *17-19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is in response to the application filed on November 24th, 2003, where applicant has filed application No. 10/720,329. The following Office Action is based on the application filed on November 24th, 2003 in which claims 1-33 and figures 1-11 are presented for examination.

Status of Claims

Claims 1 to 33 are pending, of which claims 1,17,20,21,26,29 and 33 are in independent form.

Specification

1. The abstract of the disclosure is objected to because exceeds the limit of 150 words. Applicant is reminded of the proper language and format for an abstract of the disclosure. The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. Appropriate correction is required. See MPEP § 608.01(b).

2. The Background, Summary and Detailed description of the invention in the disclosure is objected to because of the following informalities: The acronyms HTTP, UDP, TCP/IP, should be changed to Hypertext Transfer Protocol, User Datagram

Protocol (or User Data Packets) and Transmission Control Protocol/Internet Protocol and User Data Packets respectively. More so, every instance of the aforementioned acronyms should be changed in the specification.

Appropriate correction is required. See MPEP § 608.01(b) or CFR 1.71.

3. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

4. **Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Regarding claim 17, the phrase "the behavior," recited in line 2 of claim 17, renders the claims indefinite because there is insufficient antecedent basis for this limitation. It is unclear as to which application is being referred.

Re claims 18 and 19, claims 18 and 19 are dependent upon claim 17, therefore the rejections under 35 USC 112 also applies to claims 18 and19 for their dependences on claim 17.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3,8-10,12-16,20 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Parker (US 6,046,980), hereinafter Parker.

Re claim 1, Parker (US 6,046,980) discloses in **Fig 1D, a TCP/IP suite that facilitate** classification of data flows comprising

monitoring a data flow associated with a host relative to at least one behavioral attribute **[monitor network status parameters, see col. 9, lines 19-20]**;

comparing the least one behavioral attribute observed in the monitoring step to a knowledge base of at least one know application behavior pattern **[checks each level of the classification tree, matches the attributes of a given traffic class if the flow being classified matches attributes of a given traffic class, see col. 11, lines 55-58**

and Fig. 3; classifier 304]; and

classifying the data flow based on the comparing step **[the class at the level that matches determines the policy for the flow being classified, see col. 11, lines 62-63]**.

Re claim 2, Parker (US 6,046,980) discloses a method wherein

at least one behavioral attribute is packet size of the first packet in the data flow **[see col. 12, Table 2, IP address includes the packet size]**.

Re claims 3,4 and 5, said claims are dependent upon claim 1, therefore the rejections under 35 USC 102 also applies to claims 3,4 and 5 for their dependences on claim 1.

Re claim 8, Parker (US 6,046,980) discloses a method wherein

At least one behavioral attribute is the timing of the data flow relative to at least one similar data flow associated with the host **[determining a data link rate and latency period from an exchange of packet(s) between TCP endpoints, see Fig. 1E; where Tdata1 is the arrival time of first data packet and Tbase is the reference time, see col. 10, lines 32,42]**.

Re claim 9, Parker (US 6,046,980) discloses a method wherein

At least one behavioral attribute is the number of related data flows associated with the host **[The initial data packets are examined as they establish a connection.**

Parameters are developed from which RTT and Max data rate can be determined, see col. 10, lines 22-24].

Re claim 10, Parker (US 6,046,980) discloses a method wherein

At least one behavioral attribute is the timing between at least two packets in the data flow **[determining a data link rate and latency period from an exchange of packet(s) between TCP endpoints, see Fig. 1E; where Tdata1 is the arrival time of first data packet and Tbase is the reference time, see col. 10, lines 32,42]**.

Re claims 12 and 13, Parker (US 6,046,980) discloses a method wherein

At least one behavioral attribute is timing and sequence of protocol flags contained in packets of the data flow **[The SYN packets takes a finite but unknown transit time to arrive at the local TCP endpoint, where the local TCP endpoint responds with its own SYN packet (packet is of known length, issued at a know time, see col. 10, lines 37-40 and Fig. 1E; HTTP request from server to client]**.

Re claim 14, Parker (US 6,046,980) discloses a method wherein the application behavior pattern comprises

At least one instance of any one of the following: packet size pattern **[see col. 12, Table 2, IP address includes the packet size]**, a threshold information density value, a threshold inter-flow timing value **[values are obtained for serialization of n, the size of the SYN packet in response and the size of the ACK packet, see col.**

10, lines 61-63], or a threshold number of related application data flows **[TCP autobaud component 302 determines values for selectable information such as flow data rate, see col. 15, lines 24-25]**.

Re claim 15, Parker (US 6,046,980) discloses a method wherein

The application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class **[a traffic specification of a child node, such as FTP node 206 is compared with a flow specification of the new flow 300, if a match is discovered the processing in flowchart 511 is applied to the child node recursively (same traffic class), see col. 18, lines 9-13. If no policy exists, processing backtracks to a parent node and looks for a policy associated with the parent node to apply to the new flow, see col. 18, lines 21-23]**.

Re claim 16, Parker (US 6,046,980) discloses a method wherein

The application behavior pattern characterizes the first group of packets of a data flow associated with a traffic class **[all traffic which does not match any user specified traffic class falls into an automatically created default *traffic class*, which has a default policy, see col. 12, lines 66-68]** and wherein

The first group of packets are characterized in relation to at least one instance of any one of the following: a packet size pattern **[web traffic may have a service level defined for html (small files) and a separate traffic class for gif files (reserved service for larger files), see col. 13, lines30-33]**, a threshold information density

value, a threshold inter-flow timing value, or a threshold number of related application data flows **[determining an acceptable allocation of bandwidth to reserved service flows, i.e., GIR or EIR, by allocating rate for each gear 410 or 411, based upon individual flow demands, base limits and total limits, see col. 18, lines 29-33]**.

Re claim 20, Parker (US 6,046,980) discloses a method wherein

Monitoring the data flows associated with a host relative to at least one application behavior model corresponding to a traffic class [bandwidth resource needs of multiple requesting flows are reconciled in accordance with policy of each flow based upon the flow's class, see col. 4, lines 10-12];

Matching at least one of the data flows associated with the host to a traffic class if a threshold number of the data flows match a corresponding application behavior model **[available bandwidth may be allocated among flows, according to policy (and by priority) which may include any combination of GIR or EIR, see col. 4, lines 5-8]**.

Re claim 26, Parker (US 6,046,980) teaches of a method comprising

detecting a data flow in network traffic traversing a communications path, the data flows each comprising at least one packet **[Fig 1B; initiating a new flow between client and server with data objects sent to and from the network]**;

parsing explicit attributes at least one packet associated with the data flow into a flow specification **[a bandwidth manager 306 uses the policy determined by**

classifier 304 I n order to allocate bandwidth according to the service level prescribed by the policy, see col. 15, lines 33-35],

matching the flow specification to a first plurality of traffic classes, wherein the first plurality of traffic classes are each defined by one or more matching attributes **[Fig 2A and 2B; data flow assigned to TCP data flow specification, with other matching attributes such as bandwidth allocation for FTP or Web files],**

having found a matching traffic class in the matching step, associating the flow specification corresponding to the data flow with a traffic class from the first plurality of traffic classes **[see Fig 2E and 5F, where data flow is assigned to the a specification tree and subsequently assigned to root policy or a recursive child policy in the tree],**

not having found a matching traffic class in the first plurality of traffic classes matching the data flow to at least one additional traffic class, the additional traffic class defined by an application behavior pattern **[all traffic which does not match any user specified traffic class falls into an automatically created default *traffic class*, which has a default policy, see col. 12, lines 66-68],**

the application behavior pattern comprising comprises at least one instance of: a packet size pattern **[web traffic may have a service level defined for html (small files) and a separate traffic class for gif files (reserved service for larger files), see col. 13, lines30-33]**, a threshold information density value, a threshold inter-flow timing value **[values are obtained for serialization of n, the size of the SYN packet in response and the size of the ACK packet, see col. 10, lines 61-63]**, or a threshold

number of related application data flows **[determining an acceptable allocation of bandwidth to reserved service flows, i.e., GIR or EIR, by allocating rate for each gear 410 or 411, based upon individual flow demands, base limits and total limits, see col. 18, lines 29-33]**.

Claims 6,7,17,21,22 and 25 are rejected under 35 U.S.C. 102(b) as being anticipated by Aimoto et al. (US 6,144,636), hereinafter Aimoto.

Re claim 6, Aimoto et al. (US 6,144,636) discloses a method wherein

At least one behavioral attribute is the information density associated with at least one packet in the data flow **[a technique wherein information on a counter and information on a threshold value (*information density*) for each traffic class are held within the packet switch, see col. 3, lines 18-20]**.

Re claim 7, Aimoto et al. (US 6,144,636) teaches of a method wherein

At least one behavioral attribute is the information density **[information on a counter and information on a threshold value (*information density*) for each traffic class are held within the packet switch, see col. 3, lines 18-20]** associated with the first packet in the data flow **[buffers such as RIRO type input buffers and FIFO type out put buffers are included in the packet switch and an input buffer control unit determines a cell which is to be delivered, see col. 2, lines 38-41]**.

Re claim 17, Aimoto et al. (US 6,144,636) discloses in the abstract, a method wherein

Modeling the behavior of a network application to generate an application behavior pattern **[an input packet from the input port is delivered to at least one output port in accordance with address information of the input packet and connection information having been set (configured) at the time of setting the connection between the transmission source and destination]**; and

Configuring a network traffic monitoring device to classify data flows against the application behavior pattern **[an ABR congestion control function for a switch of shared buffer construction (classes) in which a cell buffer is shared by a plurality of ports bandwidth, see col. 18, lines 61-63, wherein the ABR traffic class, a bandwidth management cell periodically transmits predetermined number of data cells, see col. 2, lines 10-11]**; wherein

The application behavior pattern comprises at least one instance of any one of the following: a packet size pattern **[a Constant Bit Rate traffic class in which a fixed amount of bandwidth is continuously made available by the network to transfer cells, see col. 1, lines53-55]**, a threshold information density value **[information on a threshold value (information density) for each traffic class are held within the packet switch, see col. 3, lines 18-20]**, a threshold inter-flow timing value, or a threshold number of related application data flows **[a table having plurality of entries which illustrates behavior of congestion notification, see col. 17, lines 46-47]**.

Re claim 21, Aimoto et al. (US 6,144,636) discloses in Fig. 1 and abstract of the prior art, an apparatus wherein

A packet processor **(switch 100)** operative to detect data flows in network traffic traversing a communication path **[communication is transferred from terminal A toward terminal B via the switch, col. 9, lines 2-26]**, the data flows each comprising at least one packet **(header conversion circuit 132 and line input controller133);**

Parse at least one packet associated with a data flow into a flow specification **[input packet is delivered to at least one output port in accordance with address information of the input packet and connection info set in the packet switch at the time of connection setup]**,

A traffic classification engine operative to match the data flow to a plurality of traffic classes, at least one of the traffic classes defined by one or more application behavior patterns **[the marking mode provides at least the following apparatus in the switch for the congestion decision/notification circuit; cell number counter information, threshold value for every connection a comparator unit is also provided for every connection, connection number count, target bandwidth information register, etc. See col. 6, lines 38-46]**;

Having found a matching traffic class in the matching step **[the results of the comparator circuit in Fig. 5 is provided for every connection for deciding whether the value of a cell number counter has exceeded a threshold value information of all output ports held in the switch, see col. 6, lines 6-8]**, associate the flow

specification corresponding to the data flow with a traffic class from the plurality of traffic classes **[the bandwidth management cell which contains congestion notifications (max. bandwidth for a transmission) inserted by the decision/notification circuit decides whether the congestion notification of every connection is to performed in compliance with notification of the congested state for all output ports or, whether the congestion notification is to be immediately performed, see col. 6, lines 31-35]**.

Re claim 22, Aimoto et al. (US 6,144,636) discloses of an apparatus wherein

At least one of the plurality of traffic classes is defined by one or more matching attributes **[the marking mode provides at least the following apparatus in the switch for the congestion decision/notification circuit; cell number counter information, threshold value for every connection a comparator unit is also provided for every connection, connection number count, target bandwidth information register, etc. See col. 6, lines 38-46]**, wherein

Said matching attributes are explicitly presented in the packets associated with the data flows [**each congestion notification includes a binary marking mode (to include an explicit rate field, binary marking filed and a maximum rate field) in which the source terminal is notified of an allowed transmission, see col. 10, lines 10-14]**.

Re claim 25, Aimoto et al. (US 6,144,636) discloses of an apparatus wherein

A flow control module **[a network management device 180 utilizing a bandwidth management packet]** operative to apply bandwidth utilization controls to the data flows based on the traffic class associated with the data flows **[resources are to be managed so as to maintain a preferable communication quality (flow) even at the occurrence of congestion, also required to monitor the situation of a cell transfer (class information) within the switch, to add network switching elements, reset connections before the communication quality decreases due to traffic volume, see col. 5, lines 51-55]**.

Claims 11,18,19,23,24,27-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Bennett (US 6,122,670), hereinafter Bennett.

Re claim 11, Bennett (US 6,122,670) discloses a method wherein

At least one behavioral attribute is a sequence of protocol flags contained in packets of the data flow **[reconfigurable protocol logic subsystem, coalesces numerous operations from the various protocols which speed up the overall system processing, see col. 3, lines 50-51 and Fig. 4, protocol logic 45]**.

Re claim 18, Bennett (US 6,122,670) discloses a method wherein

The application behavior pattern comprises at least one instance of any one of the following: a packet size pattern **[source port field 310 and destination port field**

312, see Fig. 7], a threshold information density value, a threshold inter-flow timing value **[a buffer with command lists for both TCP ACK commands and for disposition queues for pending datagrams, see col. 6, lines 11-13]**, or a threshold number of related application data flows **[TCP process includes instructions for sending data to FTP client and also receiving data from FTP via buffers, see col. 4, lines 50-53 and Fig. 2B]**, an inter-packet timing value**[Datagram ID numbers, source IP addresses are passed via means of communication to the de-fragmentation lookup subsystem, see col. 9, lines 20-23 and Fig. 9, reconfigurable FPGAs 922 and 924]**, a sequence of protocol flags **[see Fig. 4, protocol logic device 45]**, an inter-packet protocol flag timing value.

Re claim 19, Bennett (US 6,122,670) discloses in Fig. 1, a TCP/IP protocol stack.

The protocol flags are TCP protocol flags **[TCP process includes *instructions* for sending data to FTP client and also receiving data from FTP via buffers, see col. 4, lines 50-53 and Fig. 2B]**.

Re claim 23, Bennett (US 6,122,670) discloses of an apparatus wherein

Flow specification contains at least one instance of any one of the following; a protocol family designation **[Fig.2A; TCP or a UDP process]**, a direction of packet flow designation, a protocol type designation **[see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client]**, a protocol type designation **[see Fig. 6; source IP address**

306 and destination IP address 308], a pair of hosts, a pair of ports a pointer to a MIME type, and a pointer to an application-specific attribute **[commands for both TCP ACK and for a disposition queue of pending datagrams; a queue of pointers to datagrams which need to be transferred to the network, see col. 6, lines 12-16]**.

Re claim 24, Bennett (US 6,122,670) discloses of an apparatus wherein

Flow specification contains, and wherein the one or more matching attributes include, at least one instance of any one of the following: a protocol family designation **[Fig.2A; TCP or a UDP process]**, a direction of packet flow designation **[see Fig. 18A and 18B, processing of incoming TCP segments constitutes a bi-directional flow of data between FTP server and FTP client]**, a protocol type designation, a pair of hosts **[see Fig. 1; nodes interconnected to form several hosts of WAN/LAN networks]**, a pair of ports **[see Fig. 7; source port 310 and destination port 312]** , a pointer to a MIME type, and a pointer to an application-specific attribute **[see Fig. 6, flags 301; fragments of original datagram and fragment offset 302; indicates bytes of original datagram length 330]**.

Re claim 27, a method corresponding to the apparatus in claim 23 is herein disclosed. Therefore, the rejection for claim 23 also applies to claim 27.

Re claim 28, a method corresponding to the apparatus in claim 24 is herein disclosed. Therefore, the rejection for claim 24 also applies to claim 28.

Re claim 29, Bennett (US 6,122,670) discloses a method comprising

detecting a data flow in network traffic traversing a communication path, the data flow comprising at least one packet **[nodes interconnected to form several hosts of WAN/LAN networks (Fig.1) where discoverable protocol is know to be TCP based on the application and FTP server (Fig.2)]**;

applying a mathematical function to at least one packet in the data flow to derive a computer value **[IP header checksum – hardware calculation – performed on receive packet to reassemble IP datagram or datagram fragment to its original structure, col. 6, lines 28-30 and Fig 6]**;

comparing the computed value to at least one traffic class, said traffic class defined, at least in part, by a required computed value **[protocol logic subsystem verifies *traffic class*; IP header and TCP segment checksums before sending datagram col. 6, lines 34-37]**.

Re claim 30, Bennett (US 6,122,670) discloses a method wherein

the required computed value is determined by applying the mathematical function to data flows know to be of the traffic class **[the header check sum is indicated by the fragment bit flag 301 and offset fragment 302 which ensures datagram validity. Based on fragment bits set, the datagram is stored in memory based on its relative offset from the beginning of the original datagram or in its own base address in memory, see col. 8, lines 34-43]**.

Re claim 31, Bennett (US 6,122,670) discloses a method wherein

the mathematical function computes a value indicating the information density of at least one packet **[based on relative offsets and partial checksums calculated, other datagrams that are received with identical identification filed 333, source and destination IP addresses, they are known to be another following fragment of a first fragment, see col. 7, lines 45-50]**.

Re claim 32, Bennett (US 6,122,670) discloses a method wherein

The required computed value is a range of values **[the reconfigurable protocol logic has memory recourses for datagram storage, and lookup tables for datagram de-fragmentation and other protocol functions, see col. 11, lines 10-15]**

Re claim 33, Bennett (US 6,122,670) discloses a method comprising

detecting a data flow in network traffic traversing a communication path, the data flow comprising at least one packet **[nodes interconnected to form several hosts of WAN/LAN networks (Fig.1) where discoverable protocol is know to be TCP based on the application and FTP server (Fig.2)]**;

applying a mathematical function to at least one packet in the data flow to derive checksum **[IP header checksum – performed on receive packet to reassemble IP datagram or datagram fragment to its original structure, col. 6, lines 28-30 and Fig 6]**;

comparing the computed checksum to the checksum value contained in at least on packet **[protocol logic subsystem verifies *traffic class*; IP header and TCP segment checksums before sending datagram col. 6, lines 34-37]**;

matching the data flow to a traffic class, wherein

the traffic class is defined at least in part by whether the computed checksum should match the checksum value in the at least one packet **[based on relative offsets and partial checksums (TCP/UDP protocol) calculated, other datagrams that are received with identical identification filed 333, source and destination IP addresses, are known to be another following fragment of a first fragment and subsequently added, see col. 7, lines 45-50]**.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Parker (US 6,046,980) in view of Bennett (US 6,122,670), herein Bennett.

Re claims 3 and 4, Parker (US 6,046,980) discloses a method meeting all preceding limitations of the parent claim, however Parker (US 6,046,980) fails to explicitly disclose of a method wherein

at least one behavioral attribute is packet size of the first packet in the data flow.

However, Bennett (US 6,122,670) teaches of a method where [**a memory 40 in a network card 2000, stores command lists for disposition queue of datagrams, see col. 6, lines 11-13. When a packet is received, network interface 50 reassembles the IP datagram or datagram fragments and then writes the corresponding datagram fragments to datagram buffer 53, see col. 6, lines 27-30. Where flag 301 and fragment offset 302 together indicate whether datagram 332 is a fragment of a larger datagram, see col. 6, lines 65-67]**. Based on the teachings of Bennett (US 6,122,670), at the time of the invention, it would have been obvious to a person in ordinary skill in the art to incorporate the network card of Bennett (US 6,122,670) in a traffic class at any level of the TCP/IP protocol or (traffic classification tree in Fig. 2C), whereby configuring a traffic class node that would specify policies by using the flag 301 and fragment offset 302 as taught by Bennett (US 6,122,670) to classify dataflow according to n-array, i.e. first, second, ...,nth datagram or datagram fragments, see col. 14, lines , Fig. 2C and Fig. 2D. Thus, it would have been obvious to one of ordinary skill in the art a the time to be motivated to incorporate the IP flag together with a fragment offset as one behavioral attribute to provide the ability to classify and search traffic based upon multiple orthogonal classification attributes.

Re claim 5, Parker (US 6,046,980) discloses a method meeting all preceding limitations of the parent claim, however Parker (US 6,046,980) fails to explicitly disclose of a method wherein

at least one behavioral attribute is packet size of plurality of packets in the data flow.

However Bennett (US 6,122,670) teaches of a method where **[an IP datagram identifier are checked against any other recently received datagrams by a de-fragmentation lookup subsystem. Either a new allocation in datagram memory 53 is created for new IP datagram identifiers, or datagram fragments are stored (accumulated) with other fragments from the same IP datagram identifier by returning the base address of the memory allocation in 53 where the previously received fragement(s) where stored, see col. 13, lines 18-24. The Protocol logic 45 sums the data (IP and TCP checksums) and transfers these sums to the accumulation register, see lines 46-48]**. Based on the teachings of Bennett (US 6,122,670), at the time of the invention, it would have been obvious to a person in ordinary skill in the art to incorporate the network card of Bennett (US 6,122,670) in a traffic class at any level of the TCP/IP protocol or (traffic classification tree in Fig. 2C), whereby configuring a traffic class node that would specify policies by using the end of the IP header of Bennett (US 6,122,670), as indication of the amount of data having been transferred equaling the value in header length field or (packet size). Thus, it would have been obvious to one of ordinary skill in the art a the time to be motivated to

incorporate the header length as one behavioral attribute to provide the ability to classify and search traffic based upon multiple orthogonal classification attributes.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Packer (US 6,038;216 A) discloses a method for explicit data rate control without data rate supervision as sliding window. The information regarding the threshold values is relevant material.

Riddle et al. (US 6,591,299 B2) discloses a method for automatically classifying packet flows for use in bandwidth allocation. The information regarding classifier and parse flow specification is relevant materials.

Wiryaman et al. (US 7,010,611B1) discloses a method for bandwidth management, receiving packets on an input port and scheduling the packets on an output port. The information regarding the bandwidth engine is of relevance.

Contacts

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rasheedat O. Koletowo whose telephone number is 571-272-9824. The examiner can normally be reached on Monday-Thursday, 7:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Coby can be reached on 571-272-4017. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Rasheedat Koletowo
R.K./r.k.
June 18, 2007

Frantz Coby
FRANTZ COBY
PRIMARY EXAMINER